Iowa Department of Public Health

Security and Confidentiality Policy

Last Reviewed: May 2010

Table of Contents

This policy is posted on the IDPH web site at the following location:
www.idph.state.ia.us/adper/idss.asp

A copy of this policy shall be made available to anyone upon request.

This policy will be reviewed annually by CADE program staff.

Purpose of the System

The Iowa Disease Surveillance System (IDSS) was developed by the Iowa Department of Public Health (IDPH) to streamline and enhance communication and collaboration between laboratory, hospital, and public health (local and state) personnel related to infectious disease surveillance and reporting (as required by Iowa Code 139A) throughout Iowa. IDSS is a tool that speeds communication regarding cases of reportable infectious disease to allow public health to respond sooner and reduce costs associated with disease reporting and surveillance. Appropriate use of IDSS consists solely of:

1) entering laboratory results related to reportable diseases,
2) entering information obtained through communication with a healthcare provider or the patient (or parent/guardian the patient),
3) review of entered information for the purpose of conducting a specific disease investigation, identifying clusters of infectious disease, identifying relationships between cases, identifying disease trends to direct disease prevention efforts.
4) review of entered information for the purpose of evaluating and improving disease surveillance activities.
5) creating de-identified, system-generated reports for public release to increase awareness of infectious disease as part of either ongoing general disease prevention messages or a specific disease prevention message.
6) transmission of de-identified data to the Centers for Disease Control and Prevention.
7) transmission of completed records via a secure transport mechanism to other states when an out of state referral is necessary.

Privacy

The information contained in the IDSS database is confidential patient information. The protection of an individual's right to keep this information private and confidential is a priority of the Iowa Department of Public Health, Center for Acute Disease Epidemiology. Persons with information contained in the system can be assured of the following:

- Information in the system will only be used in ways that are consistent with the purpose of the system.
- Only authorized users will have access to information in the system.
- Enrolled users shall not release patient identifiable data obtained from the system.
- Only de-identified information such as disease counts contained in system-generated reports will be released publicly.

Confidentiality

This confidentiality policy governs the collection, storage and disclosure of information in IDSS. All forms of access and disclosure are covered by this policy, electronic, written or printed materials, and verbal communications.

Access to and Disclosure of System Information

All individually identifiable information that is stored in the IDSS database, paper-based records, and electronic records are considered to be confidential information and shall not be disclosed by the authorized user except as authorized by state or federal law. If an individual can be identified or inferred through a reasonable examination of the information, this information is protected by this policy.

Authorized System Users

All authorized users must read, agree and adhere to the terms specified in this document. The user will then be granted authorized access to the system through IDSS enrollment with IDPH. Only authorized users may provide information to the system or obtain information from the system.

Authorized users may access individual case records in their jurisdiction only for the purpose of conducting or assisting with an investigation of infectious disease. Users must exercise due diligence when accessing records to assure that the record that is opened is for the appropriate case (to prevent any breach of confidentiality). A breach of confidentiality is the disclosure of information stored in the IDSS database (including paper-based and electronic records) to a third party, without consent, court order, or other specific legal authority.

Authorized users may access and use this information exclusively for the reasons listed in the section titled "Purpose of the System" (page 3). Access or use of system information for any other purpose is strictly prohibited and is considered a breach of confidentiality.

Some examples of prohibited use are:

- To deny benefits or services to an individual or family
- To locate an individual for billing or marketing purposes
- For law enforcement purposes
- To track undocumented immigrants

Retrieval of Patient Information

In addition to the ability to access individual patient records in the system, authorized users may also retrieve a complete record of a patient's information and demographics for patients in their jurisdiction. An authorized user's right to access individual patient information is limited to patients who are under their care or jurisdiction.

Storage and Disposal of Confidential Information

Authorized users shall store personally identifiable information printed or copied from the system in a secure manner such as in locked cabinets. When information is no longer needed in paper form, the authorized user shall shred all documentation. CD's, disks and any other version of media that contains identifiable information that is no longer needed shall be destroyed.

Requests for Aggregate Information

All information contained in the IDSS is the property of IDPH. Authorized users, researchers or others may request aggregate data from the system. All requests for aggregate data are subject to approval, may consist of de-identified information only and must be referred to the IDSS Coordinator at the address listed below:

IDSS Coordinator
Center for Acute Disease Epidemiology
Iowa Department of Public Health
Lucas Building
321 E. 12th Street
Des Moines, IA 50319
Fax: 515-281-5698
e-mail:IDSS@idph.state.ia.us

Data Retention

Information submitted to the system will be retained according to Iowa Department of Public Health policy.

Confidentiality Agreements

The individual who signs the IDSS Enrollment Application is responsible for assuring that they have read, understand and agree to abide by this policy.

Prior to being added to the system as an authorized user, each individual must indicate their agreement to the terms of this policy by printing their name and providing a signature on the IDSS Security and Confidentiality Agreement Form that is on page 11 of this document.

Each authorized user must review the IDSS Security and Confidentiality Policy and renew their signature on the IDSS Security and Confidentiality Agreement on an annual basis.

A copy of the IDSS Security and Confidentiality Agreement Form for each authorized user must be kept on file within the participating facility and must be available for inspection upon request.

Security

Security refers to the measures that the IDSS users will take to protect the data from unauthorized access or unwanted change or loss. It also includes procedures such as audit trails, physical access controls, user I.D.s, passwords, access levels, and data recovery policies.

Authorized users of the system are required to exercise reasonable administrative, technical, and physical safeguards to (1) ensure the integrity and confidentiality of system information; (2) to protect against reasonably anticipated threats to the security of system information including unauthorized use or disclosure of the information.

The individual who signs the IDSS Security and Confidentiality Agreement is responsible for assuring that they have read, understand and agree to abide by this policy, the Third Party Agreement, and the New User Token Request form.

Encryption

The transmission of system information via the Internet to and from the user's computer and the system database is protected through the use of 256-bit encryption technology. All of the information in the data stream is encrypted.

Decryption by the user's computer can only occur when the appropriate software is installed (the software installation is protected by a registration key that is securely delivered to enrolled facilities), and when the software is accessed by means of a valid user I.D. and password combination.

Secure server access

Physical access to the servers that store system information is controlled through locked and alarmed entryways at the Iowa Department of Public Health (IDPH). IDPH Network Administrators are automatically notified whenever anyone enters the server room.

External electronic access to the system servers is actively protected through the use of firewall technology.

Server Reliability

All servers that are used by the IDSS are monitored by an automated attendant 24 hours a day, seven days a week. IDPH Network Administrators are automatically notified via a wireless statewide network at the first sign of malfunction.

Most updates or repairs can be completed without interruption of service to the system; however, when scheduled maintenance is needed it will be completed between the hours of 6 p.m. on Monday to 6 a.m. on Tuesday. Whenever possible, system users will be notified via email message at least 24 hours in advance of any maintenance activity that may include service interruption.

Network / Communications Reliability

IDPH maintains service agreements on most routing and switching equipment that is in use by the system. These agreements specify 24 hour repair or replacement on all critical infrastructure items.

Redundant hardware is onsite for items not covered by service agreements. This hardware can be used to restore services within 24 hours.

Data Backup and Recovery

The system database is automatically backed up to tape once every 24 hours, these tapes are scheduled for a 12 week rotation. Once a week, the database is copied to tapes which are stored off site in a secure facility, and are rotated every two weeks. Month end copies are stored off site for one year.

Complete recovery of system data from tape backups can be completed within 24 hours.

User ID's and security tokens

Each individual who accesses system information must have a unique User I.D., password and security token combination.

The User I.D. identifies the individual who is authorized to access system data while the password provides verification of the given user's identification. The security token provides an independent, second layer of authentication.

Authorized users are not permitted to share their User I.D., password or security token with anyone else even on a temporary basis. There may be a nominal fee (currently $100 for 5 years of service) associated with each security token payable to IDPH upon request for enrollment. This fee may be waived under certain circumstances. For example, the fee is waived for replacement of tokens that have not been damaged or misused, but no longer function properly.

The IDSS local administrator at each facility with access to the IDPH Application Setup Web, www.iowadiseasesurveillance.org/setup, also has access to forms used in managing tokens at their local facility. There are four forms available to manage four different situations efficiently:

- The Token Change form communicates information to update the existing token user's name or reassign a token to a new user.
- The Token Inactivate form communicates information to inactivate a user or their access to IDSS.
- The Token Replacement form communicates information to replace a lost or damaged token.
- The Token New IDSS form communicates a request for a new IDSS user and is used to link a current token to IDSS or request a new token for a new user.

Installation of IDSS

Installation of the IDSS client application on each authorized user's PC is the responsibility of local administrators at each facility. Only local administrators are given necessary login credentials to download and register the IDSS client application from a secure web site. Since sharing a user ID, password, and token is forbidden, the local administrator must assist with each IDSS installation for each local user at their facility. It is acceptable for the local administrator to gain assistance from local information technology staff for installation purposes. It is neither necessary for nor will Information technology staff be provided authorized access to IDSS, even temporarily, for installation of the client application.

In order to establish a unique ID for system users, the driver's license number is requested as part of user information. This information can be accessed only by authorized IDSS System staff. This information is subject to the same confidentiality and disclosure rules as any other information in the system.

Inactivating User Accounts

Authorized local administrators at enrolled offices or clinics are responsible for immediately deactivating user accounts for individuals who no longer are employed by that facility or who no longer need to have access to system information. A form to facilitate inactivation of user accounts is available at the same web site from which the application is downloaded. Local administrators are provided information about this web site individually.

Audit Trails

The system employs detailed auditing regarding the access of system data. Audit trails permit the identification of individual users who open system records and who make changes to those records.

Software and Registration Keys

All media (CD-ROMs, diskettes, tapes, etc.) that contain a copy of the IDSS software must be stored in a secure location.

Registration keys that are issued to enrolled offices or clinics must also be kept in a secure location separate from the software.

Penalties

A breach of this privacy, confidentiality and security policy by an authorized user may result in the temporary or permanent exclusion of the user and /or their clinic or office from the system.

While a breach of confidentiality or security is under investigation, the IDSS staff reserves the right to suspend all system access by a clinic or office or individual users thereof.

Any suspected violation of this policy should be immediately reported to the IDSS staff by phone at 1-800-362-2736 and followed up within 48 hours in writing to the address below:

Iowa Department of Public Health
Center for Acute Disease Epidemiology
IDSS Program
Lucas State Office Building
321 East 12th Street
Des Moines, Iowa 50319

Unauthorized disclosure or access of system information may also result in criminal or civil penalties.

Glossary

Access is the authorization and capability to enter and/or review system data.

Authorized users are those individuals or organizations that require regular access to infectious disease-related information on a specific individual to perform one of the activities listed under Purpose of the System. Authorized users may include health care providers, hospital infectious disease staff, laboratory staff, and public health department staff (state and local).

Breach of Confidentiality is the disclosure of information stored in the IDSS database (including paper-based and electronic records) to a third party, without consent, court order, or other specific legal authority.

CADE is the Center for Acute Disease Epidemiology, a Bureau of the Iowa Department of Public Health.

Confidentiality is the treatment of information that an individual has disclosed in a relationship of trust with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure.

Confidentiality agreement is a written statement, dated and signed by an individual which certifies that the individual has read a copy of the confidentiality policy, understands the terms, and agrees to comply with the policy.

Enrollment application defines the terms under which individuals and organizations become authorized users; it includes obligations and responsibilities of both parties.

De-identified information is health information from which personal identifiers have been removed, masked, encrypted or otherwise concealed, such that the information can not reasonably be expected to identify individual patients. For example, a de-identified report may contain the name of the disease and a county in which the disease occurred, but all information that could be used to identify a patient has been removed from the report.

Disclosure refers to the release of information to and from the system.

Individually identifiable information is information that identifies the individual, or can be used to identify the individual.

Jurisdiction refers to the patient records over which an agency's or facility's infectious disease reporting and investigation responsibility extends. Jurisdiction extends to each user affiliated with a given agency or facility. The system automatically limits jurisdiction based on agency or facility and user security level. All identifiable patient information is limited by jurisdiction for each user of a given agency or facility.

Local administrators are those users at the local hospital, laboratory, or public health agency level that have been granted credentials to access the secure web site from which IDSS is downloaded and installed. There is a local administrator at each facility that has access to IDSS and they must be involved with every installation of IDSS at their facility.

Privacy is the legal right of an individual to limit access by others to some aspect of their person.

Re-disclosure is the disclosure by a third party recipient of disclosed health information with the authorization of the person.

Security encompasses a set of technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction.

Security token is a physical device used to generate a changing value assigned to a specific authorized IDSS user that must be used to access the IDSS.

User is a person that is permitted to view, add and edit system records. Has the ability to create patient and general reports.

Iowa Disease Surveillance System (IDSS)

Security and Confidentiality Agreement

Facility or Agency: _____

Participant Name: _____
Last Name *First Name* *Title*

Address: _____
Street

_____
City *State* *Zip Code*

*Phone: ( )*_____ *Fax: ( )*_____ *Email Address:*_____

Supervisor's Name: _____
Last Name *First Name* *Title*

*Supervisor's Phone: ( )*_____ *Email Address:*_____

The complete Iowa Disease Surveillance System Security and Confidentiality Policy is posted on the IDPH Web site at the following location: www.idph.state.ia.us/adper/idss.asp. It is understood that the participant signing this agreement has read, understands, and agrees to abide by the entire Iowa Disease Surveillance System Security and Confidentiality policy.

In order to use IDSS, I specifically agree to the following:

IDSS and Iowa Department of Public Health (IDPH) Responsibilities

Hardware: *The IDPH is responsible for the maintenance of database and file server(s) that support the IDSS application. IDPH personnel are responsible for ensuring that this equipment is available to participants during routine use hours. Routine system maintenance will be scheduled for Mondays at 6 p.m. to Tuesdays at 6 a.m.; the system may not be available during these periods. Most routine maintenance will require less than the listed 12 hour period; however, participants should not assume that access will be possible during these times.*

Database: *The IDPH is responsible for the routine maintenance and backups of the IDSS database. All appropriate measures will be taken to assure the integrity and security of the IDSS database.*

Software: *The IDPH is responsible for providing access to the IDSS application for enrolled participants to participate in statewide disease surveillance. The application remains the property of the IDPH, and may not be copied or transferred to anyone other than the enrolled participant. IDPH provides the IDSS software to the participant free of charge (see security under Participant Responsibilities for potential token service fee). Technical support for the IDSS application will be provided by the IDPH.*

Security: *The IDPH is responsible for the physical security of the IDSS database and related server(s). All appropriate measures will be taken to protect against unauthorized access and to provide the appropriate physical environment for the file server(s) and other associated equipment. A security token is required for every user to access IDSS.*

Confidentiality: *The IDPH is responsible for the enrollment of appropriate participants for IDSS. Enrollment is limited to users in eligible hospitals, laboratories, and local public health agencies. The IDPH is responsible for monitoring the use of IDSS by enrolled participants to protect against inappropriate use of the system. The IDPH retains the right to require periodic re-enrollment of all participants.*

Support *The IDPH is responsible for the technical support of the IDSS application. IDPH personnel will be assigned during normal business hours to provide assistance with troubleshooting the IDSS application as well as answering user questions. This "Help Desk" can be accessed by participants through the toll-free Disease Reporting Hotline (800) 362-2736, pager at 515-235-0262, or through e-mail to IDSS@idph.state.ia.us. The IDPH does not provide direct technical support for the participant's computer hardware or network services.*

The IDPH will maintain an "online" help manual, training manual and support web site for the use of participants. Participants will be permitted to download a printable version of the online help manual.

(Continued)

Iowa Disease Surveillance System (IDSS)

Security and Confidentiality Agreement

Participant Responsibilities

Hardware: *The participant is responsible for the purchase and maintenance of all computer hardware related to the use of the IDSS application. This hardware must meet the minimum specifications as follows: Windows 2000, XP, or later; 600 MHz AMD or Intel processor (1.0 GHz recommended); 256 MB RAM (512 MB + recommended); 800 MB hard disk space (includes 200 MB for .Net framework); 800X600 256 color display.*

Software: *Full functionality of IDSS requires Microsoft .Net Framework 1.1(later versions will not interfere, but .Net Framework 1.1 is required), Microsoft Web Service Enhancements (WSE) 2.0 service pack 3, and Adobe Reader 7.0 or later.*

Communication: *The participant is responsible for obtaining an Internet connection for every computer from which they will use the IDSS application. An active Internet connection is required by the application. Each entity must be able to support individual registration keys for each facility.*

Application: *The participant is responsible for the appropriate use of the IDSS application. Appropriate use of IDSS consists solely of: entering laboratory results related to reportable diseases; entering information obtained through communication with a healthcare provider or the patient (or parent/guardian the patient); review of entered information for the purpose of conducting a specific disease investigation, identifying clusters of infectious disease, identifying relationships between cases, and identifying disease trends to direct disease prevention efforts; review of entered information to evaluate and improve disease surveillance; creating de-identified, system-generated reports for public release to increase awareness of infectious disease as part of either ongoing general disease prevention messages or a specific disease prevention message; transmission of de-identified data to the Centers for Disease Control and Prevention; transmission of complete records via a secure transport mechanism to other states when an out of state referral is necessary. The following uses of the IDSS application are inappropriate and are prohibited: its use to deny services to an individual or family; locate or identify individuals for billing, marketing, or law enforcement purposes; track undocumented immigrants; or any other use IDPH determines to be inconsistent with the purpose and function of IDSS.*

Security: *It is the responsibility of the participant to control physical access to the IDSS application which provides access to the IDSS database. The participant shall take reasonable measures to limit such access to persons who have the authority to view patient/client information. A security token is required for every user to access IDSS. There may be a nominal fee (currently $100 for 5 years of service) associated with each security token payable to IDPH upon request for enrollment. This fee may be waived under certain circumstances. The participant understands and agrees that all passwords are confidential and that no password or security token is to be shared. The participant must assist IDPH to assure that all users within their office/agency have a unique User Id, password, and security token used to access the IDSS application. All users within an office/agency must enroll directly with IDPH.*

Participants are responsible for contacting IDPH for prompt removal of the User account for individuals that are no longer authorized to access the IDSS application. An e-mail should be promptly sent to IDSS@idph.state.ia.us when an IDSS user is no longer authorized to access the system.

Data entry: *The participant is responsible for the timely entry of infectious disease reports and investigation information into the IDSS database.*

Confidentiality: *IDSS information, including identifying and demographic data maintained in IDSS, is confidential and shall not be disclosed by the participant, except as authorized by state or federal law.*

Fees: *The participant will not impose a charge or fee to the patient/client for the use of IDSS.*

Policy: *The participant agrees to comply with the IDSS Security and Confidentiality Policy posted at* ***www.idph.state.ia.us/adper/idss.asp****.*

Violation: *Any violation of this agreement may result in the permanent exclusion of the participant from the use of the system, and/or other civil or criminal penalties.*

The Participant or the Iowa Department of Public Health may terminate this agreement at any time for any reason by sending a written notice of termination to the other party. This record is to be submitted to and kept on file at the Iowa Department of Public Health.

_____ _____

Participant signature *Date*

Please return to the attention of the IDSS Coordinator at:

By mail: Iowa Department of Public Health
Center for Acute Epidemiology
321 E. 12th Street
Des Moines, IA 50319-0075

OR by fax:
(515) 281-5698

For IDPH use only

Date enrolled in IDSS: _____.
Organization number: _____.